16 STRON EKSTRA

VPN I BEZPIECZEŃSTWO Ć

WINDOWS | SMARTFON | TELEWIZOR | KONSOLA

PARTNER WYDANIA:
Surfshark®

Komputer Świat

VPN

PRYWATNOŚĆ I BEZPIECZEŃSTWO

WINDOWS | SMARTFON | TELEWIZOR | KONSOLA

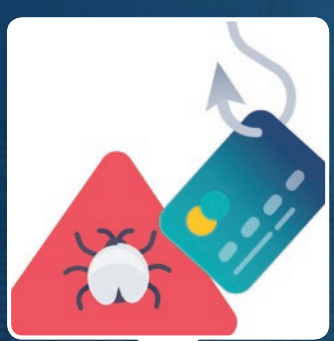
- Zablokuj szpiegowanie w Windows
- Zadbaj o prywatność w przeglądarkach
- Zabezpiecz połączenie przez VPN

WARTO WIEDZIEĆ:

Szyfrowanie łącza udaremnia **ataki hakerskie**

Ochrona przed manipulacją i reklamami

Kradzież tożsamości: jak się zabezpieczyć



Jak uniknąć phishingu i naciągania

DLACZEGO TRZEBA CHRONIĆ SWOJĄ PRYWATNOŚĆ W SIECI

Internet to tylko narzędzie – sieć przenosząca informacje. Dowolne informacje, również takie, których publikowania byśmy sobie nie życzyli. ***Tak jak w domu zamykamy drzwi przed obcymi, tak w sieci warto zadbać o prywatność***

Internet jest w tej chwili najważniejszym medium komunikacyjnym ludzkości. Pozwala nam uzyskać dostęp do wiadomości ze świata z dowolnej dziedziny, zapewnia dostęp do wielu usług rozrywkowych, daje możliwość kontaktu z bliskimi i wiele więcej. Łatwość transferu danych to jednak także poważne zagrożenie dla naszej prywatności.

Prywatność online nie istnieje?

Wielu tak sądzi. Istotnie, podczas normalnego korzystania z komputera, smartfona, tabletu czy nawet połączonych z internetem innych urządzeń, takich jak na przykład czytnik e-booków, konsola do gier czy telewizor smart TV, bardzo łatwo zostawiamy wiele śladów naszej aktywności w sieci. Odwiedzając niemal każdy serwis online, zapewne wielokrotnie byliśmy bombardowani prośbami o akceptację plików cookies. Ciasteczka to elementy pozwalające identyfikować naszą cyfrową tożsamość na wielu witrynach. Z jednej strony pozwala to dostarczać nam odpowiednich treści, a niekiedy wręcz warunkuje funkcjonowanie jakiejś spersonalizowanej usługi. Z drugiej niemal automatyczna akceptacja ustawień prywatności danego serwisu oznacza zgodę na personalizowanie treści reklamowych. Z pewnością wielokrotnie tego doświadczyliście, na przykład szukacie nowego laptopa dla dziecka do nauki. Już po krótkim surfowaniu w poszukiwaniu rzeczonego sprzętu, odwiedzając jakikolwiek serwis z reklamami Google AdSense, zobaczycie… reklamy laptopów właśnie.

Algorytmy sięgają dalej

Macki algorytmów śledzących poczynania użytkowników korzystających z usług online nie ograniczają się tylko do analizy naszej aktywności na komputerze podczas na przykład poszukiwania jakiegoś towaru czy usługi. Jedziecie odwiedzić rodzinę, ktoś z waszych bliskich ma problemy ze słuchem, dyskutujecie o rozwiązaniu problemu. Nie bądźcie zaskoczeni, gdy surfując później po Facebooku czy wiadomościach Google, zobaczycie reklamy… aparatów słuchowych. Inny przykład, pandemia, siedzenie w domu. Przytyło się wam? Czy nie zwróciliście uwagi, że jakoś częściej zaczęły wam się pojawiać reklamy promujące różne sposoby odchudzania? Wierzcie nam – to nie przypadek. Każdy smartfon czy laptop ma mikrofon. Każdy smartfon czy laptop ma kamerę. Sami zresztą z pewnością wielokrotnie udostępnialiście znajomym zdjęcia, dzieliliście się wrażeniami z podróży, rozmawialiście online o różnych problemach.

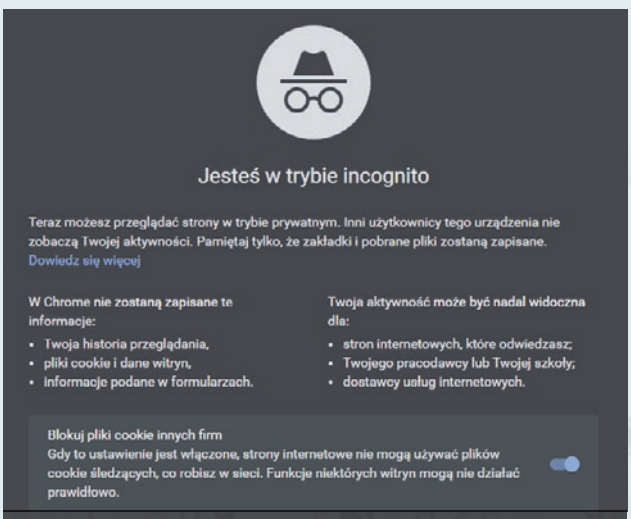
Profile konsumenckie online

Wiemy już, że podczas normalnego korzystania z internetu jesteśmy w zasadzie pod stałą obserwacją. Jednak należy wyraźnie rozróżnić marketingowe profilowanie użytkownika (personalizacja treści reklamowych) od śledzenia obywateli czy zagrożeń wynikających z ujawnienia naszej prywatności. Profilowanie marketingowe wydaje się tu stosunkowo niewinne. W końcu, co złego w tym, że wyświetlają nam się reklamy rzeczy, których akurat szukamy? Jednak algorytmy nie mają sumienia i ludzkiej moralności. Dorosły internauta jest w stanie oprzeć się nachalnej reklamie, ostatecznie ją wyłączy. A dzieci? Ochrona dzieci i ich prywatności w sieci to odrębny problem,

UODO RADZI, CO ZROBIĆ W RAZIE KRADZIEŻY TOŻSAMOŚCI

Otrzymałeś wezwanie do zapłaty od operatora telekomunikacyjnego, z którym nie podpisywałeś umowy? Bank wzywa cię do zapłaty zaległej raty kredytu, o którym nie masz pojęcia? To efekty kradzieży tożsamości. W internetowym serwisie Urzędu Ochrony Danych Osobowych pod adresem: **https://uodo.gov.pl/pl/138/1222** znajdziesz informacje, jak postępować w takich przypadkach.

Google jest najbardziej funkcjonalną wyszukiwarką świata także dlatego, że... dużo o nas wie. Jeżeli nie chcesz udostępniać swoich danych wyszukiwarce, korzystaj z takich, które ich nie zbierają, na przykład Startpage czy DuckDuckGo



Korzystając z wbudowanego w wiele przeglądarek trybu prywatnego (w Chrome nazywa się on trybem Incognito), znacząco ograniczamy możliwość profilowania marketingowego podczas surfowania i śledzenie naszej aktywności w sieci

PARTNER WYDANIA:
Surfshark®

Fot. Andranik Hakobyan/iStockphoto.com

Jednym z najlepszych sposobów na ochronę prywatności jest użycie VPN

na który powinniśmy również zwracać uwagę. Dziecko nie będzie psychicznie tak odporne na przekaz reklamowy jak osoba dorosła.

Agencje wywiadowcze

Jeżeli chodzi o wywiad. Możemy założyć, że agencje wywiadowcze, gdy tylko zechcą, mogą wiedzieć o nas praktycznie wszystko. Już w 2013 roku Washington Post i brytyjski The Guardian ujawniły szczegóły dotyczące tajnego programu PRISM prowadzonego przez amerykańską agencję NSA. PRISM to tajny program, który umożliwia NSA dostęp do danych jakiegokolwiek amerykańskiego operatora/usługodawcy w internecie. Co nas mogą obchodzić amerykańskie usługi? Cóż, korzystacie przecież z Google, Microsoftu, Apple'a, Facebooka, prawda? Oczywiście NSA nie jest zainteresowane tym, że lubisz przeglądać zdjęcia kotków w internecie albo że wysłałeś znajomej przepis na sernik. Inwigilacja ma na celu ochronę bezpieczeństwa Stanów Zjednoczonych i walkę z terroryzmem. Przynajmniej oficjalnie.

Cyberprzestępcy i kradzież tożsamości

Najgroźniejszą konsekwencją niedbałości o własną prywatność w internecie jest kradzież naszej tożsamości przez cyberprzestępców. W takim przypadku jesteśmy bowiem narażeni na realne straty finansowe. Cyberprzestępcy kradną cyfrowe tożsamości użytkowników najczęściej po to, by za pomocą wykradzionych danych popełniać dalsze przestępstwa w imieniu niczego nieświadomych użytkowników internetu. Więcej w ramce UODO radzi, co zrobić w razie kradzieży tożsamości.

Czy możemy coś zrobić?

Czy to znaczy, że możemy machnąć ręką i „niech się dzieje, co ma się dziać"? Absolutnie nie. Każdy użytkownik internetu ma do swojej dyspozycji szereg narzędzi, za pomocą których może mieć wpływ na to, jakie dane i komu udostępnia. Oczywiście naiwnością byłoby sądzić, że przeciętny Kowalski za pomocą powszechnie dostępnych narzędzi jest w stanie dać odpór wyspecjalizowanym agencjom wywiadowczym, ale już jakiekolwiek utrudnienie w zdobyciu naszych danych cyberprzestępcom może spowodować, że poszukają oni po prostu łatwiejszego celu. Sugerowane metody ochrony prywatności online wymieniamy w ramce obok. Na kolejnych stronach naszego dodatku rozwijamy tę kwestię.

Afera PRISM pokazała, że NSA może słuchać wszystkiego i wszystkich

OCHRONA PRYWATNOŚCI – JAK SIĘ BRONIĆ

Każdy internauta dysponuje łatwo dostępnymi i relatywnie prostymi narzędziami w konfiguracji, pozwalającymi skutecznie zwiększyć anonimowość podczas korzystania z internetu.

- **VPN** – bardzo skuteczne rozwiązanie zapewniające bezpieczne i anonimowe połączenie z internetem. Bezwzględnie zalecamy używanie VPN podczas korzystania z internetu przez publiczne sieci Wi-Fi (na przykład na lotniskach, w hotelach, kawiarniach itp.). Więcej o tym rozwiązaniu na kolejnych stronach.
- **Sieć Tor** – to niejako sieć w sieci. Tor bazuje na tak zwanym trasowaniu cebulowym, w którym ruch pomiędzy poszczególnymi węzłami jest szyfrowany i anonimizowany. Korzystanie z Tora jest o tyle proste, że możemy na przykład anonimowo surfować za pomocą dedykowanej przeglądarki Tor Browser.
- **Odpowiednia konfiguracja przeglądarki** – paradoksalnie znaczną pomoc w ochronie prywatności może nam zapewnić odpowiednia konfiguracja naszej przeglądarki internetowej. Na przykład korzystając z trybu incognito w Google Chrome czy okna prywatnego w Firefoxie, przeglądarka nie zapisze i nie wyśle do jakiejkolwiek odwiedzanej strony żadnych plików cookies ani nie przechowuje historii odwiedzin, co pozwala w znacznym stopniu ograniczyć na przykład profilowanie treści marketingowych.
- **Szyfrowanie** – metoda tyleż skuteczna, co po prostu uciążliwa przy paranoidalnym podejściu do prywatności. Niemniej możliwe jest korzystanie z szyfrowanych sieci (VPN) przeglądarek (Tor) czy komunikatorów (na przykład Signal – z tego komunikatora korzystał Edward Snowden.
- **Korzystanie z wyszukiwarek internetowych** niegromadzących danych o użytkowniku, na przykład DuckDuckGo (www.duckduckgo.com) czy Startpage (www.startpage.com)
- **Uzbrojenie przeglądarki w rozszerzenia informujące o trackerach** (mechanizmach śledzących użytkownika na odwiedzanych przez niego stronach) z funkcją blokowania ich działania (na przykład przeglądarka Vivaldi blokuje reklamy i trackery marketingowe).

PRYWATNOŚĆ W USTAWIENIACH WINDOWS

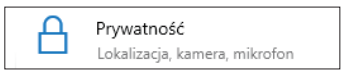
Warto znać najważniejsze ustawienia systemu mające znaczenie dla naszej prywatności. *Dzięki nim można ograniczyć zbieranie o nas danych przez system, dostosować uprawnienia programów oraz wyłączyć kamerę i mikrofon*

ŚLEDZENIE LOKALIZACJI

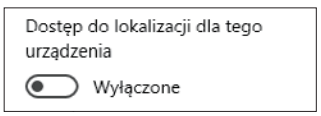
Domyślnie Windows 10 na bieżąco zapisuje informacje na temat lokalizacji użytkownika (ma to znaczenie w przypadku użytkowników laptopów). Z jednej strony pozwala to na odnalezienie sprzętu, z drugiej jednak służy do dostosowywania wyświetlanych nam reklam, które są dopasowane do miejsca naszego pobytu. Możemy łatwo wyłączyć śledzenie naszej lokalizacji.

1 Uruchamiamy **Ustawienia systemowe**.

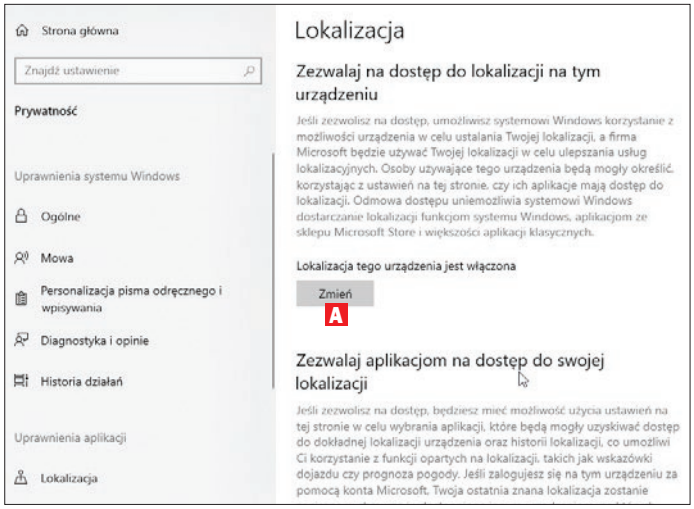
2 Następnie klikamy na pozycję **Prywatność**.



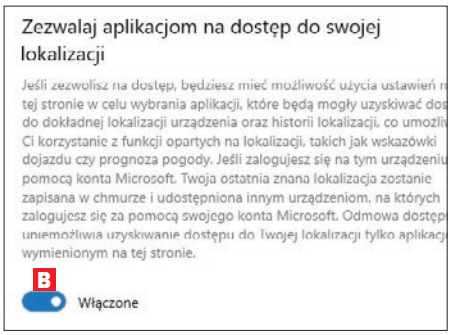
3 Teraz po lewej stronie klikamy na **Lokalizacja**, a po prawej na **Zmień** i zmieniamy opcję dostępu na **Wyłączona**.

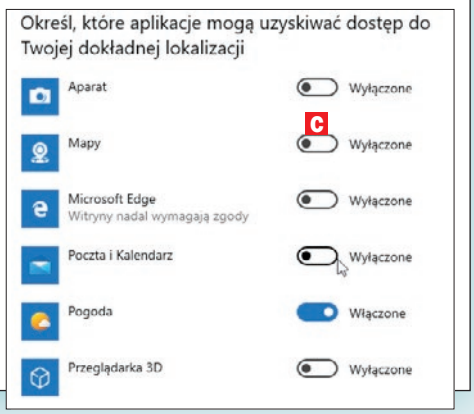


4 Jeśli z różnych względów nie chcemy całkowicie wyłączać opcji lokalizacji, możemy pozostawić ją włączoną **A** i ręcznie kontrolować dostęp wybranych aplikacji do usług lokalizacyjnych. Najpierw musimy zezwolić aplikacjom na dostęp do lokalizacji **B**.



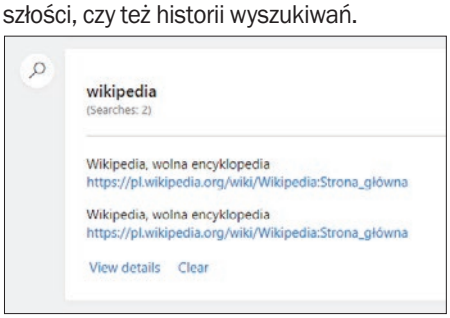
5 Następnie przewijamy widok niżej i ręcznie przyznajemy dostęp do naszej lokalizacji każdej aplikacji lub go blokujemy **C**.





BLOKUJEMY I CZYŚCIMY HISTORIĘ DZIAŁAŃ

Windows od 2018 roku ma niezbyt znaną funkcję **Historia działań**. Pozwala ona na sprawdzanie aktywności użytkownika, jego lokalizacji oraz czynności wykonywanych na komputerze. Dodatkowo łączy informacje z konta użytkownika na różnych urządzeniach, co pozwala na sprawdzenie plików, z którymi pracowaliśmy na innych urządzeniach w przeszłości, czy też historii wyszukiwań.

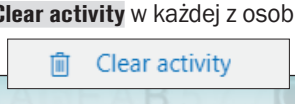


1 Dostęp do tej funkcji znajdziemy, klikając na **Ustawienia**, **Prywatność**, **Historia działań**.

2 Jeśli nie chcemy, aby dane z naszego konta były zbierane i wysyłane, należy wyłączyć opcje zachowywania historii aktywności **A** oraz wysyłania **B**.

3 Następnie musimy jeszcze wyczyścić historię działań. W tym celu klikamy na link w dolnej części ekranu – **Zarządzaj moimi danymi aktywności konta Microsoft** **C**.

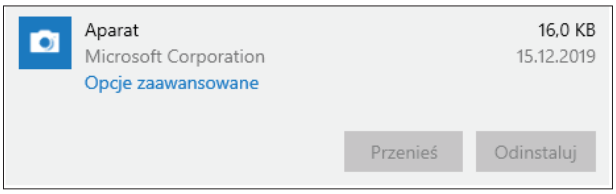
4 Po zalogowaniu się na stronę z danymi dotyczącymi naszego profilu wystarczy przejść przez kolejne kategorie, klikając na opcję **Clear activity** w każdej z osobna.



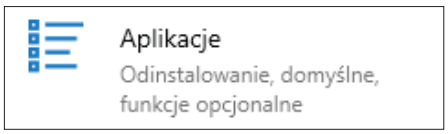
PARTNER WYDANIA:
Surfshark®

KONTROLUJEMY UPRAWNIENIA APLIKACJI

Domyślnie system Windows ma aktywowanych wiele uprawnień aplikacji, które mogą naruszać prywatność użytkowników. Warto sprawdzić, które aplikacje mają jakie uprawnienia i wyłączyć te, które mogą naruszyć naszą prywatność.

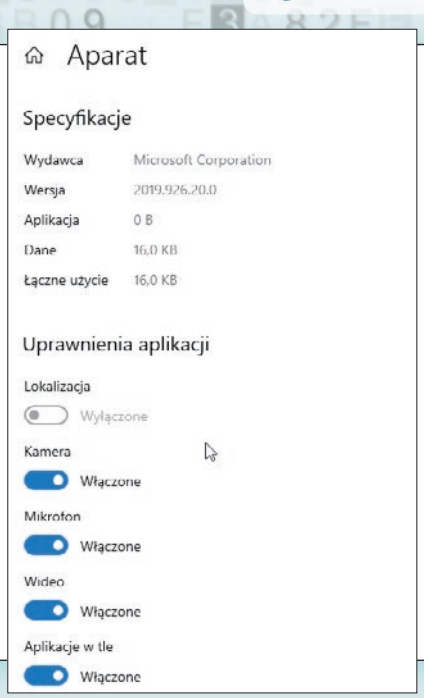


1 Przechodzimy do Ustawień systemu, następnie klikamy na **Aplikacje**.



2 Po prawej stronie na liście wybieramy poszczególne aplikacje i klikamy na **Opcje zaawansowane**. Aplikacje, przy których nie ma linku **Opcje zaawansowane**, nie korzystają z dodatkowych uprawnień w systemie Windows.

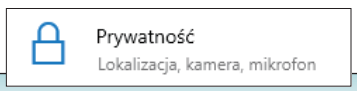
3 W polu **Uprawnienia aplikacji** decydujemy, jakie uprawnienia ma mieć dana aplikacja.



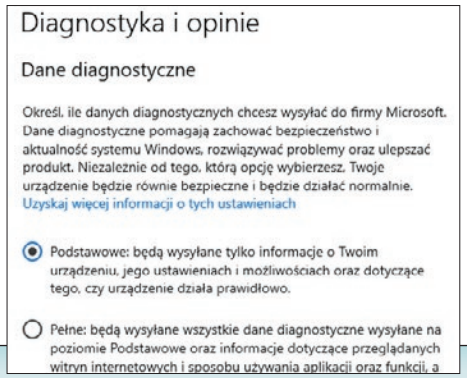
USTAWIENIA ZBIERANIA DANYCH DIAGNOSTYCZNYCH

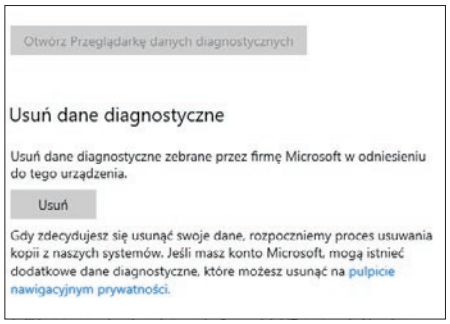
Windows zgodnie z domyślnymi ustawieniami zbiera i wysyła do firmy Microsoft pełne dane diagnostyczne – nie tylko informacje o urządzeniu, jego ustawieniach i możliwościach, ale także dotyczące między innymi przeglądanych witryn, sposobu używania aplikacji i funkcji czy kondycji komputera i wykonywanych na nim działań. Warto ograniczyć poziom zbieranych o nas danych i usunąć te już zapisane. Oto jak to zrobić.

1 Przechodzimy do Ustawień systemu, następnie klikamy na **Prywatność**.



2 Po lewej stronie klikamy na **Diagnostyka i opinie**. Po prawej stronie zaznaczamy **Podstawowe** zamiast **Pełne** i przewijamy widok do pozycji **Usuń dane diagnostyczne**, a potem klikamy na polecenie **Usuń**. Proces usuwania takich danych może potrwać kilka dni.

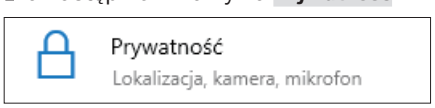




WYŁĄCZAMY DOSTĘP DLA KAMERY I MIKROFONU

Kluczową rolę dla naszej prywatności mają mikrofon i kamera wbudowane w większość laptopów. Jeśli niebezpieczne aplikacje mają do nich dostęp, może to stanowić zagrożenie, gdyż w czasie rzeczywistym mogą nas nagrywać lub słuchać naszych rozmów, a zapisane dane wysyłać na serwery swoich twórców. Oto jak sprawdzić, które aplikacje korzystają z kamery i mikrofonu.

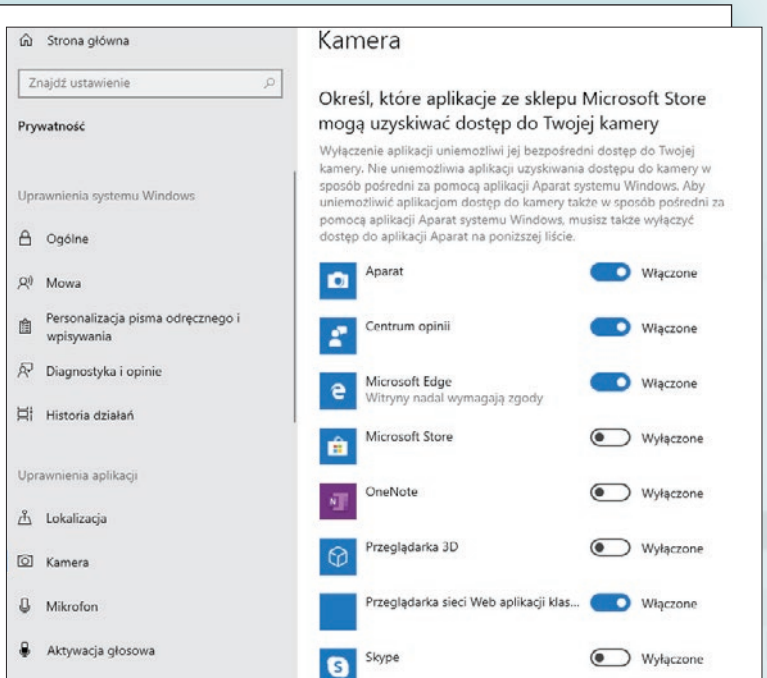
1 Przechodzimy do Ustawień systemu, a następnie klikamy na **Prywatność**.



2 Następnie po lewej stronie klikamy na **Kamera** i przewijamy widok do listy aplikacji.

Następnie kontrolujemy każdą aplikację osobno i nadajemy jej odpowiednie uprawnienia. W każdej chwili możemy je zmienić, dlatego też jeśli nie jesteśmy pewni jakiejś aplikacji, najlepiej jest wyłączyć jej dostęp do naszej kamery.

3 Dokładnie te same kroki należy wykonać dla ustawień mikrofonu.



ZABEZPIECZENIA PRZEGLĄDARKI

Do popularnych przeglądarek, takich jak Google Chrome, Mozilla Firefox czy Opera, możemy dodać ***specjalne rozszerzenia, które zwiększają bezpieczeństwo oraz chronią przed potencjalnymi zagrożeniami.*** *Oto jak to zrobić i na jakie rozszerzenia zwrócić uwagę*

JAK ZAINSTALOWAĆ DODATKI W PRZEGLĄDARKACH

CHROME

Zobaczmy, jak dodawać rozszerzenia w najpopularniejszej w Polsce przeglądarce Google Chrome.

INSTALUJEMY ROZSZERZENIA

W oknie Chrome musimy kliknąć na trzy kropki w prawym górnym rogu, a następnie przesunąć kursor na **Więcej narzędzi** i kliknąć na **Rozszerzenia**. Po lewej stronie ekranu klikamy na trzy kreski i na samym dole wybieramy opcję **Otwórz Chrome Web Store**. Teraz możemy skorzystać z pola wyszukiwania dodatków. Po kliknięciu na wybrany dodatek wystarczy jeszcze tylko kliknąć na **Dodaj do Chrome**, a po chwili pokaże się okno z prośbą o potwierdzenie. Po potwierdzeniu dodatek zostanie zainstalowany.

FIREFOX

Firefox to lubiana przeglądarka z rozbudowanym trybem prywatnym z ochroną przed śledzeniem. Jest znany z tego, że jego możliwości można rozbudowywać dzięki dodatkom.

INSTALUJEMY ROZSZERZENIA

Po uruchomieniu Firefoxa klikamy w prawym górnym rogu okna na trzy kreski i z listy wybieramy opcję **Dodatki**.
Następnie po lewej stronie klikamy na **Pobierz dodatki**, a po prawej na **Znajdź więcej dodatków**. Korzystając z pola wyszukiwania, znajdujemy potrzebny nam dodatek. Po wybraniu dodatku klikamy na **Dodaj do Firefoxa**, a po chwili przyznajemy uprawnienia, klikając na **Dodaj**.

OPERA

Opera to warta uwagi przeglądarka z ciekawymi autorskimi usprawnieniami. Ma między innymi wbudowaną blokadę reklam i darmowy VPN.

INSTALUJEMY ROZSZERZENIA

W oknie przeglądarki klikamy w lewym górnym rogu na **Menu**, przesuwamy kursor na **Rozszerzenia** i klikamy na **Pobierz rozszerzenia**. Wpisujemy w pole wyszukiwania nazwę dodatku lub wyszukujemy go w katalogu ogólnym. Jeśli zdecydujemy się go dodać, klikamy na zielony przycisk **Dodaj do Opery**. Instalacja przebiega automatycznie i nie musimy już nic potwierdzać. W celu skorzystania z dodatku wystarczy kliknąć na jego ikonę po prawej stronie paska adresowego.

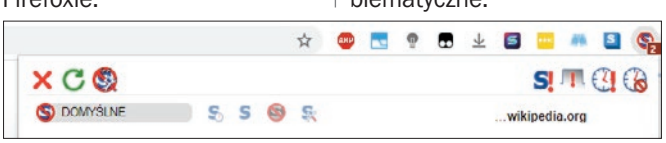
TE DODATKI POPRAWIAJĄ NASZĄ PRYWATNOŚĆ

NOSCRIPT

Bardzo przydatny dodatek, którego zadaniem jest blokowanie skryptów JavaScript i apletów Java, Flash, Silverlight. Zapewnia to większe bezpieczeństwo, zwłaszcza jeśli odwiedzamy mało znane i potencjalnie niebezpieczne witryny, ponieważ blokada skryptów wykonywalnych chroni nas przed wyskakującymi oknami lub fałszywymi nakładkami na różnych witrynach. To rozwiązanie to niezbędne wyposażenie przeglądarki każdego świadomego użytkownika internetu. Zainstalujemy je w Chromie oraz Firefoxie.

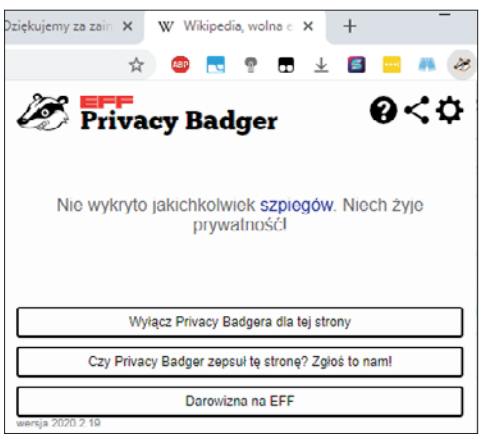
1 Po zainstalowaniu dodatku, by uzyskać do niego dostęp, należy kliknąć na jego ikonę na pasku adresowym przeglądarki.

2 W oknie możemy kontrolować, jakie elementy mogą być wyświetlane, a jakie mają być blokowane. Dzięki bardzo dobrej domyślnej konfiguracji właściwie nie trzeba zmieniać żadnych opcji, aby bezpiecznie korzystać z przeglądarki, dlatego rozwiązanie to polecane jest nawet dla zupełnie początkujących osób, dla których konfigurowanie ustawień może być problematyczne.



PRIVACY BADGER

Privacy Badger to dodatek jedyny w swoim rodzaju. Powstrzymuje wszelkie kody ze stron internetowych przed podpinaniem nam znacznika śledzącego. Taki znacznik pozwala firmom na tworzenie naszego profilu poprzez informacje uzyskane w wyniku śledzenia naszych wyszukiwań w sieci i odwiedzanych stron. Dodatek ten po wykryciu śledzącego kodu wyłącza go, a firma, która nas śledzi, otrzymuje informacje, że zniknęliśmy z sieci.



Privacy Badger dopiero po kilku sesjach z przeglądarką dostosuje swoje ustawienia i filtry do naszego trybu przeglądania. Możemy też wyłączać lub włączać elementy kontrolowane.

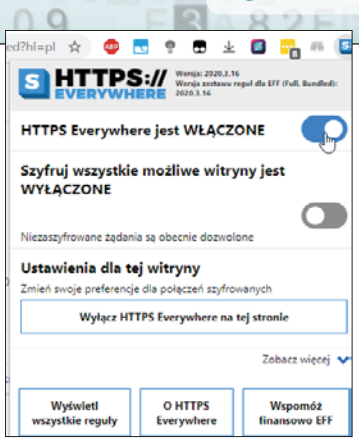
HTTPS EVERYWHERE

Jest to bardzo prosty dodatek, który pomoże poprawić nasze bezpieczeństwo w sieci. Często witryny mogą mieć zaszyfrowaną tylko stronę główną, podczas gdy domyślnie podstrony będą wczytywały się jako zwykłe HTTP bez możliwości ochrony danych, które odbieramy i wysyłamy. Dodatek wymusza stosowanie protokołu HTTPS, jeśli tylko dana domena na to pozwala. (Zawsze sprawdzajmy, korzystając z poczty lub bankowości internetowej, czy jesteśmy połączeni protokołem HTTPS).

KORZYSTANIE Z DODATKU

1 Przy pierwszym uruchomieniu zostaniemy zapytani, czy chcemy korzystać z usług **SSL Observatory**. Jest to usługa, która pomaga wykryć, czy nasza przeglądarka nie została zaatakowana. Wystarczy kliknąć na **Tak**.

2 Upewniamy się, czy funkcja **HTTPS Everywhere** jest włączona. Teraz w trakcie przeglądania witryn automatycznie wszelkie odnośniki, na które możemy kliknąć, będą uruchamiane przez protokół HTTPS, jeśli tylko jest taka możliwość.



BEZPIECZNY KOMUNIKATOR

Jeśli niepokoi nas to, że WhatsApp czy Messenger mogą podsłuchiwać nasze rozmowy ze znajomymi, to czas, by zmienić komunikator. ***Komputer Świat proponuje przesiadkę na Signal, którego celem jest dbanie o poufność konwersacji***

KOMUNIKATOR SIGNAL

Android* iPhone*

Signal to dość nietypowy komunikator. Zanim zaczniemy w pełni z niego korzystać w środowisku Windows, wymagana jest jego instalacja na smartfonie. Potrzebny link w postaci kodu QR wyświetlony zostanie bezpośrednio w interfejsie programu. Po chwili konfiguracji będziemy mogli korzystać z bezpiecznego komunikatora na naszym komputerze. Signal pozwala na wysyłanie wiadomości tekstowych, obrazów, komunikację głosową, a nawet wideoroz mowy. Cała komunikacja jest zabezpieczona i nikt nie będzie mógł nas podsłuchać ani sprawdzić, o czym piszemy. Dodatkowo możemy ustawić czyszczenie historii rozmów, dzięki czemu starsze wiadomości będą same znikały.

KONFIGURUJEMY PROGRAM DO PRACY

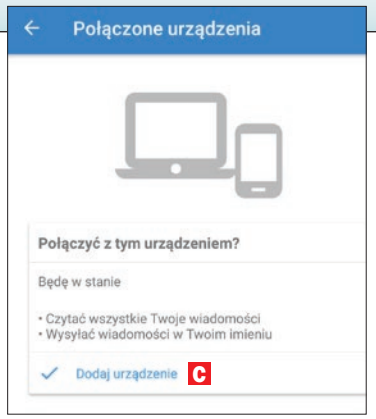
1 Zanim uruchomimy Signal na komputerze, musimy zainstalować go na naszym smartfonie, łatwo go znaleźć w sklepie z aplikacjami. Możemy skorzystać z kodów. Następnie uruchamiamy aplikację na smartfonie i postępujemy zgodnie z instrukcjami na ekranie.

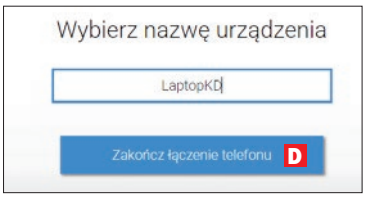
2 Dodajemy nasz komputer do aplikacji Signal. W smartfonie naciskamy kolejno **Ustawienia**, **Połączone urządzenia** A, **+**. Uruchamiamy aplikację Signal na komputerze i skanujemy kod QR B widoczny na ekranie komputera.

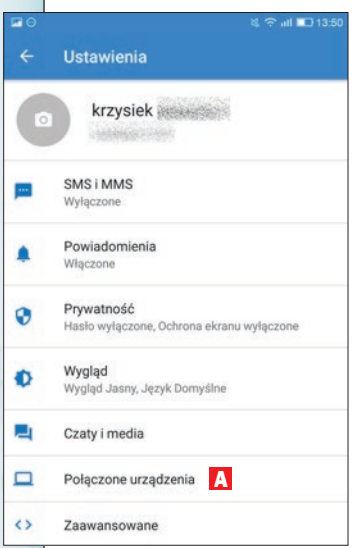
3 Naciskamy **Dodaj urządzenie** C w smartfonie.

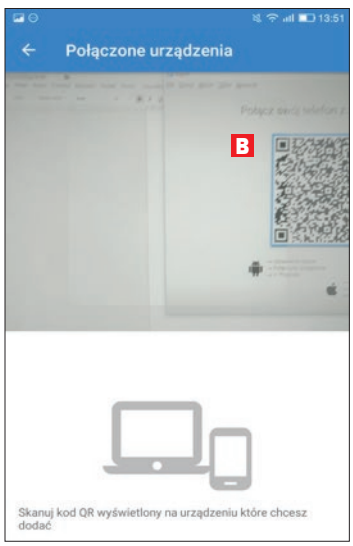
4 Na komputerze wprowadzamy nazwę urządzenia, z którego korzystamy, i klikamy na **Zakończ łączenie telefonu** D.

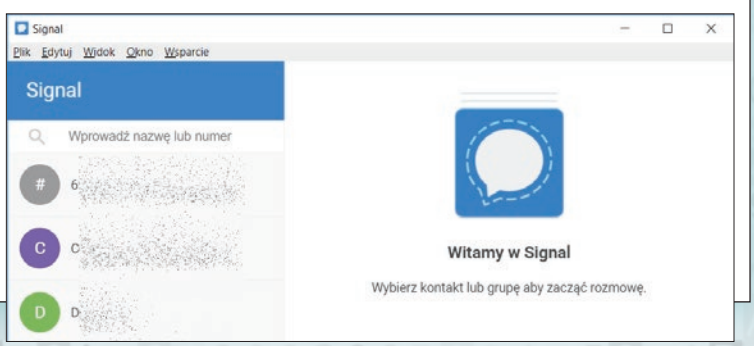
5 Teraz będziemy mogli komunikować się ze znajomymi, wykorzystując nie tylko smartfon, ale i komputer, co może być wygodne podczas dłuższej pracy, a nasze dane będą bezpiecznie szyfrowane.











* Kod QR szybko przenosi na stronę, skąd można pobrać aplikację. W iPhonie skanujemy go aplikacją aparatu, użytkownicy Androida mogą użyć dowolnej aplikacji QR pobranej z Google Play

VPN – SKUTECZNA OCHRONA PRYWATNOŚCI

Jednym z najlepszych pod każdym względem sposobów na ochronę naszej prywatności podczas korzystania z jakichkolwiek zasobów internetowych jest technika VPN. ***Komputer Świat wyjaśnia, co to jest VPN, jak działa, a także na czym polega wyższy poziom bezpieczeństwa, anonimowości i ochrona prywatności użytkownika za pomocą tej techniki***

Agresywna reklama, służby wywiadowcze, wścibscy internetowi giganci, cyberprzestępcy – jest bardzo wiele dobrych powodów, aby w internecie zadbać o ochronę własnej prywatności. Jedną z najskuteczniejszych metod takiej ochrony jest korzystanie z usług VPN. Zacznijmy od tego, co to w ogóle jest.

Czym jest VPN?

Nazwa VPN pochodzi z anglojęzycznego zwrotu Virtual Private Network (Wirtualna Sieć Prywatna), co poniekąd już wyjaśnia sposób, w jaki ta usługa działa. Użytkownik, który zdecyduje się na skorzystanie z VPN, dysponuje jakby wirtualnym tunelem na dane pomiędzy własnym komputerem, smartfonem czy innym urządzeniem wpiętym do globalnej sieci a jakimkolwiek zdalnym serwisem, firmową siecią czy inną dowolną usługą online. Zresztą VPN jest również znany pod inną nazwą: połączenia tunelowe – co dość dobrze oddaje istotę rzeczy. Takie ukryte, tunelowe połączenie może być realizowane pomiędzy użytkownikiem a siecią (na przykład w scenariuszu, gdy zdalny pracownik potrzebuje uzyskać bezpieczny dostęp do zasobów sieci firmowej, które z oczywistych względów wymagają wyższego poziomu ochrony) bądź pomiędzy dwoma odrębnymi sieciami (na przykład pomiędzy dwoma oddziałami firmy, które w ten sposób mogą funkcjonować tak, jakby znajdowały się wewnątrz jednej, wewnętrznej sieci firmowej).

Bezpłatne publiczne sieci Wi-Fi mogą być bardzo niebezpieczne, korzystanie z VPN może w takim przypadku bardzo skutecznie podnieść poziom bezpieczeństwa

Jak działa VPN?

Istotą działania tej usługi jest tworzenie tunelowego, szyfrowanego połączenia pomiędzy dwoma punktami w sieci. To użytkownik decyduje, z czym chce się połączyć, więc od jego

ONAVO I FACEBOOK

Nieistniejąca już dziś izraelska usługa **Onavo**, przejęta przez Facebooka w 2013 roku, oficjalnie funkcjonowała jako VPN. Niestety, w rzeczywistości Facebook wykorzystywał Onavo do zbierania danych o użytkownikach, którzy – z samego faktu, że korzystali z VPN – tych danych ujawniać nie chcieli. Działania społecznościowego giganta były na tyle perfidne, że na mobilnym kliencie Facebooka przez jakiś czas widoczny był przycisk „zwiększający ochronę", de facto uruchamiający zewnętrzną aplikację Onavo Protect, która choć formalnie działała jak VPN, to w rzeczywistości dostarczała Facebookowi znacznie dokładniejszych danych o użytkownikach niż ci udostępniają podczas zwykłego surfowania. Trudno się dziwić, że Onavo przez wiele niezależnych narzędzi zabezpieczających szybko został sklasyfikowany jako spyware. Jeżeli duży gracz w branży IT, żyjący z analizy danych i reklam internetowych (Facebook, Google, Yahoo itp.), proponuje wam „darmowy VPN", lepiej mieć się na baczności. Generalnie pamiętajmy o złotej zasadzie: nie ma darmowych obiadów.

PARTNER WYDANIA:
Surfshark®

VPN CHRONI NAS NIE TYLKO PODCZAS SURFOWANIA ZA POMOCĄ KOMPUTERA, RÓWNIEŻ GDY KORZYSTAMY ZE SMARTFONA I USŁUG ONLINE

WYBÓR OPERATORA VPN MA ZNACZENIE, BO NIE KAŻDY ZAPEWNIA ODPOWIEDNI POZIOM BEZPIECZEŃSTWA

strony korzystanie z VPN nie jest bardziej uciążliwe od zwykłego surfowania po internecie. Zalety korzystania z VPN uświadomimy sobie, stosując analogię do ruchu na autostradzie – zresztą internet jest często nazywany światową infostradą. Wyobraź sobie, że jedziesz motocyklem po autostradzie – z łatwością można stwierdzić, skąd wyruszyłeś (źródło danych), z czym jedziesz (jakie dane), dokąd zmierzasz (z kim się łączysz) i po co (jakie dane cię interesują). VPN tworzy tunel. Dla ciebie niewiele się zmienia, dalej masz połączenie, ale z zewnątrz nie widać, czym jedziesz, skąd, dokąd i po jakie paczki (dane). VPN, tworząc tunel, a właściwie całą gęstą sieć tuneli o niewidocznej zawartości dla osób postronnych, zapewnia dwie istotne rzeczy: ukrywa, kto i z kim się łączy (anonimizacja transmisji danych) oraz szyfruje przesyłane dane (zwiększa bezpieczeństwo przesyłanych informacji). Obserwatorzy z zewnątrz mogą co najwyżej „widzieć" sam tunel (fakt, że jest jakieś połączenie), ale skąd i dokąd przepływają dane i jakie są to dane – już nie. To wie tylko sam użytkownik oraz… operator usługi VPN, który odpowiada za ukrywanie adresu IP, lokalizacji i innych danych użytkownika podczas korzystania z usługi.

Wybór VPN ma znaczenie

Usługodawca VPN to niejako zarządca tunelu infostrady. Jako zarządzający ruchem w tunelu siłą rzeczy wie, co się w nim dzieje, dlatego odpowiedni wybór rzetelnego i wiarygodnego usługodawcy ma bardzo istotne znaczenie. Przykładem pokazującym, do czego może prowadzić nieroztropność w tej kwestii, jest niedziałający już serwis VPN Onavo – patrz ramka Onavo i Facebook. Wybierając konkretnego usługodawcę, zawsze należy sprawdzić opinie na jego temat. Na kolejnych stronach naszego dodatku pokazujemy wam, jak używać i skonfigurować na różnych urządzeniach bezpieczną usługę VPN realizowaną przez SurfShark.

ZALETY I WADY VPN

Zalety VPN:

- Cały ruch generowany przez ciebie (niezależnie od tego, z czego korzystasz: komputer, smartfon, konsola itp.) jest szyfrowany, co utrudnia śledzenie i zakłócanie komunikacji z zewnątrz.
- VPN umożliwia znacznie bezpieczniejsze korzystanie z publicznych sieci Wi-Fi.
- Odpowiednio skonfigurowany VPN pozwala surfować anonimowo.
- Anonimowy ruch pozwala zniwelować dyskryminowanie ze względu na lokalizację: blokadę regionalną dostępu do jakiejś usługi, czy na przykład manipulacje cenowe, czyli wyświetlanie wyższych cen towarów i usług użytkownikom surfującym z bogatszych regionów.
- VPN umożliwia blokowanie trackerów reklamowych, samych reklam, a także ataków sieciowych i złośliwego oprogramowania.

Wady VPN

- Wybór operatora VPN może mieć kluczowe znaczenie dla bezpieczeństwa ruchu.
- Operatorzy VPN wykorzystują wiele różnych protokołów o różnym stopniu bezpieczeństwa – podstawowym wyborem zawsze powinien być protokół OpenVPN, jeżeli usługodawca oferuje przestarzały protokół PPTP, to… wybierzmy innego usługodawcę.
- Transfer danych za pośrednictwem VPN jest najczęściej wolniejszy niż podczas zwykłego połączenia przy tym samym łączu.

JAK VPN ZAPEWNIA ANONIMOWOŚĆ

- Korzystając z VPN, łączysz się najpierw z jednym z serwerów usługodawcy VPN, niezależnie od tego, jaki faktycznie docelowy adres wybrałeś.
- Usługodawca VPN szyfruje połączenie i ukrywa adres źródłowy klienta (czyli twój), następnie przekierowuje zanonimizowane już pakiety do adresu docelowego.
- Serwer docelowy otrzymuje pakiety dane, ale nie jest w stanie rozpoznać ich źródła, zamiast naszego adresu podstawiany jest adres serwera VPN.
- Podstawiany zamiast naszego adres IP najczęściej jest zmienny – usługodawcy VPN dysponują zazwyczaj gęstą siecią serwerów rozmieszczonych w różnych lokalizacjach.

Fot. Scanrail, Bigtunaonline/iStockphoto.com

POZNAJ SURFSHARK

Wiemy już, że VPN to jeden z najlepszych sposobów na korzystanie z globalnych zasobów sieci z dobrą ochroną prywatności użytkownika. Poziom bezpieczeństwa jest jednak silnie uzależniony od wyboru konkretnego usługodawcy VPN. ***W tym numerze Komputer Świat poleca serwis SurfShark, dowiedzmy się dlaczego***

SurfShark to względnie nowy gracz na rynku VPN. Paradoksalnie to zaleta. Co istotne – niejedyna w przypadku tej usługi. Mimo niedługiego stażu na rynku (firma powstała w 2018 roku) SurfShark podszedł do sprawy ambitnie, w ciągu zaledwie roku firma uruchomiła ponad 1700 serwerów w 63 krajach świata. Dziś ich liczba to ponad 3200 w 65 krajach. To ma o tyle znaczenie, że infrastruktura usługodawcy im jest bogatsza, tym więcej wirtualnych lokalizacji może być podstawianych dla korzystającego z VPN użytkownika, który chce zachować bezpieczeństwo i anonimowość podczas surfowania.

Dobra usługa VPN nie powinna znacząco ograniczać prędkości transmisji danych

Firma odporna na zakusy rządów na dane

Istotny jest też jeszcze jeden szczegół: SurfShark ma siedzibę na Brytyjskich Wyspach Dziewiczych (BWD) i choć jest to terytorium zamorskie Zjednoczonego Królestwa, to BWD ma własne prawo i własny system sądownictwa i w przeciwieństwie do bardzo wielu krajów świata, nie ma tam prawnie wymuszanych mechanizmów ujawniania danych przez operatorów internetowych. Oznacza to, że SurfShark może działać w pełni anonimowo z poszanowaniem litery prawa i żaden rząd żadnego kraju nie może żądać od usługodawcy ujawnienia danych użytkowników. Zresztą nie jest to możliwe ze względów technicznych – serwery SurfShark nie przechowują danych na trwałych nośnikach, przetwarzanie danych odbywa się w pamięci RAM serwerów, a – jak wiadomo – jest to pamięć ulotna. Wystarczy odłączenie zasilania i po danych nie ma śladu.

Brak logowania danych

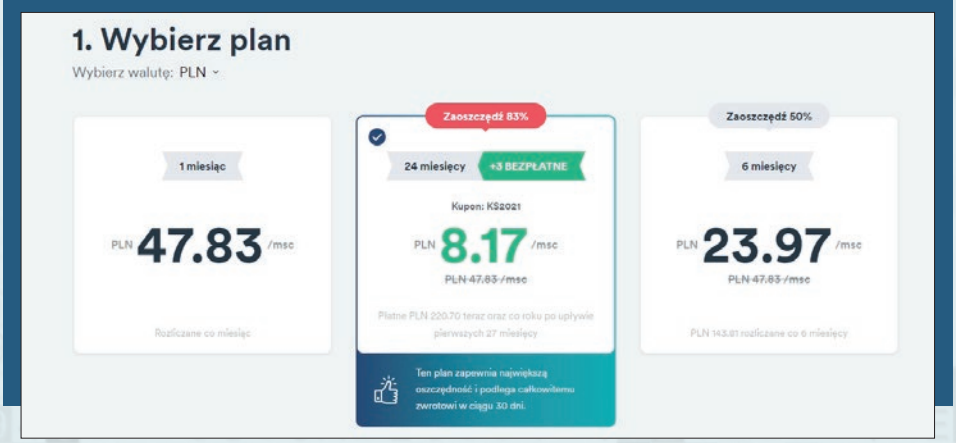
Zarzutem formowanym w stronę wielu usługodawców VPN jest to, że przechowują oni dane, które przetwarzają. W rezultacie poziom ochrony użytkownika realnie spada, bo wystarczy skuteczny atak na bazę usługodawcy i całą anonimowość diabli biorą. W przypadku SurfShark jest inaczej. Firma nie przechowuje żadnych danych, które mogą zidentyfikować konkretnego użytkownika. Nie są przechowywane żadne adresy IP (zarówno przychodzące, jak i wychodzące), historia odwiedzin serwisów za pośrednictwem VPN, historia pobierań danych czy przeprowadzonych transakcji, żadnych śladów. Firma określa to polityką bez rejestrowania.

Szeroki zakres usług

Poziom anonimowości i bezpieczeństwo to jedno, ale usługa VPN powinna też być funkcjonalna. Chodzi o to, by użytkownik za pośrednictwem VPN uzyskiwał dostęp do zasobów, z których chce bezpiecznie korzystać. W przypadku SurfShark ten warunek jest spełniony, usługa SurfShark VPN obsługuje streaming, co w połączeniu z fałszowaniem lokalizacji pozwala użytkownikowi uzyskać dostęp do zasobów regionalnie blokowanych. Na przykład oferta Netflix w USA jest znacznie bogatsza niż w Polsce, inny gracz na rynku streamingu mediów – amerykańskie Hulu – w ogóle nie jest dostępny w Polsce. Za pośrednictwem VPN użytkownik może „udawać", że jest na przykład w Stanach Zjednoczonych, otrzymując dostęp do danej usługi. Ciekawostką jest to, że Netflix nauczył się blokować niektórych operatorów VPN, jednak w przypadku SurfShark tak nie jest.
Za pośrednictwem SurfShark VPN możliwe jest również bezpieczne korzystanie z sieci

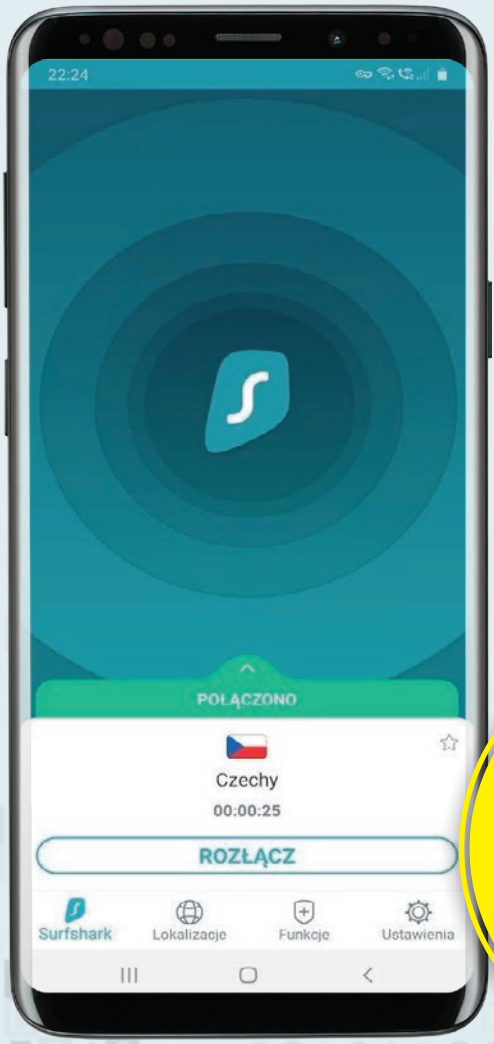
SURFSHARK PRZYGOTOWAŁ SPECJALNY RABAT DLA CZYTELNIKÓW KOMPUTER ŚWIATA!

Czytelnicy Komputer Świata mogą zabezpieczyć wszystkie swoje urządzenia i sieć domową dzięki usłudze SurfShark. Operator przygotował zniżkę aż 85 procent od cen standardowych! Informacje, jak skorzystać z promocji, znajdziemy na stronie 16 tego Raportu.



Usługa SurfShark dysponuje ponad 3200 serwerami w 65 krajach świata

P2P, bo ruch współdzielony (esensja P2P) jest obsługiwany przez SurfShark VPN. Usług oferowanych w ramach SurfShark VPN jest więcej, wymieniamy je w ramce Zalety SurfShark VPN.



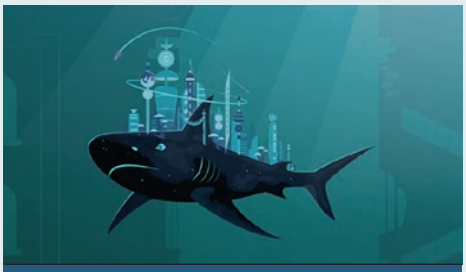
Duża szybkość transmisji

Nie jest tajemnicą, że VPN zmniejsza szybkość transmisji danych. W przypadku bezpłatnych usług VPN różnice są często drastyczne, możesz mieć w domu szybkie światłowodowe łącze, a po wypróbowaniu darmowego VPN dowolna strona będzie ładować się z prędkością, jakiej doświadczaliśmy w czasach wdzwanianego dostępu do internetu. To może skutecznie zniechęcić. Niemniej to nie wada VPN jako takiego, lecz usługodawcy. W przypadku SurfShark VPN tego problemu nie ma, sprawdziliśmy to. Owszem, szybkość transmisji nieco spada (tym bardziej, im dalej zlokalizowane są serwery, które „udają" naszą lokalizację), ale to czysta fizyka. Ważniejsze jest to, że nawet przy spadku szybkości połączenia komfort korzystania z usług online pozostaje na wysokim poziomie – wciąż możemy oglądać strumieniowo filmy w wysokiej jakości.

Brak limitu urządzeń

Kolejną zaletą opisywanej usługi jest brak limitu urządzeń należących do użytkownika, które mają się łączyć z internetem za pośrednictwem SurfShark VPN. Opłacając usługę, nie mamy żadnych ograniczeń, zarówno co do liczby, jak i typu urządzeń. Może to być komputer stacjonarny z Windows, laptop, komputer z systemem Apple, smartfon lub tablet z Androidem, sprzęt mobilny Apple, a nawet telewizory smart TV czy konsole do gier.

ZA POMOCĄ KLIENTA SURFSHARK VPN NA SMARTFONIE MOŻEMY „UDAWAĆ" NIEMAL DOWOLNĄ LOKALIZACJĘ DOSŁOWNIE JEDNYM DOTKNIĘCIEM EKRANU



ZALETY SURFSHARK VPN

- Dostępne rozszerzenia dla popularnych przeglądarek (Chrome, Firefox)
- Działa na urządzeniach mobilnych
- Nieograniczona ilość urządzeń na jednego użytkownika
- Obsługuje współdzielenie plików w sieciach P2P
- Pomoc techniczna w formie czatu dostępna 24/7
- Funkcja blokowania reklam CleanWeb
- Polityka braku logów umożliwiających identyfikację jakiegokolwiek użytkownika usługi
- Wyłącznik awaryjny
- Bardzo mocne szyfrowanie (algorytm AES-256-GCM)
- Funkcja Multihop – ekstremalne utrudnienie prób śledzenia użytkownika (korzystanie z kilku serwerów VPN w trakcie jednej sesji)
- Duża szybkość połączeń

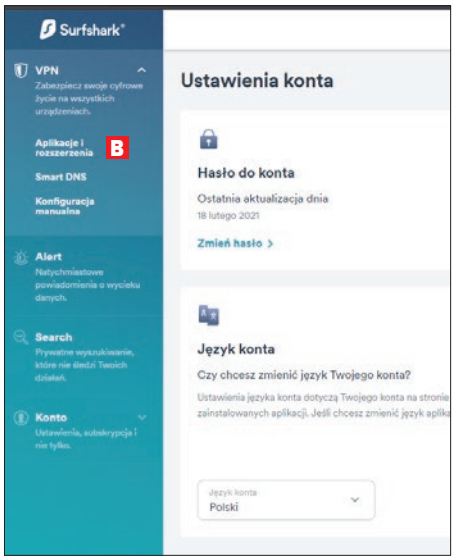
Fot. Allvisionn, NanoStockk/iStockphoto.com

JAK KORZYSTAĆ Z VPN NA KOMPUTERZE I SMARTFONIE

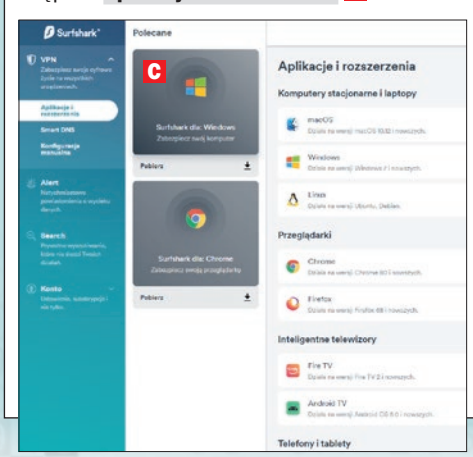
Wiesz już, że VPN to bardzo skuteczny sposób na zapewnienie sobie anonimowości i ochrony przed szpiegującymi reklamami czy innymi zagrożeniami z sieci. Komputer Świat pokaże, ***w jaki sposób rozpocząć korzystanie z usługi VPN zarówno na komputerze, jak i smartfonie*** *w oparciu o usługę SurfShark VPN*

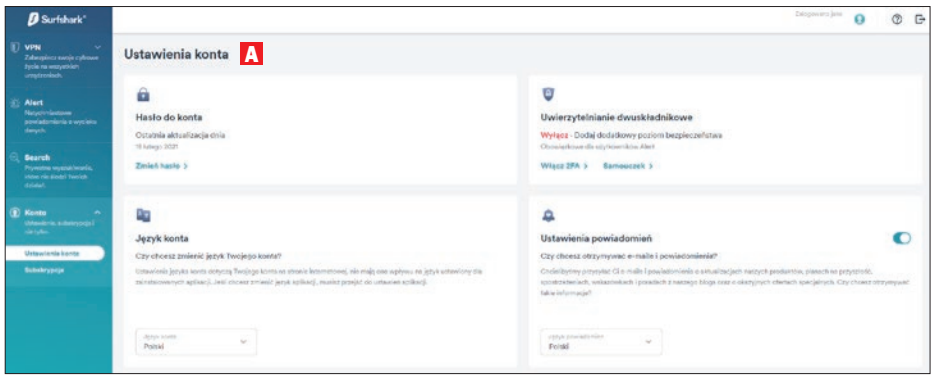
VPN NA KOMPUTERZE Z WINDOWS

Zacznijmy od konfiguracji usługi SurfShark VPN na komputerze z systemem Windows. Zaczynamy od aktywacji usługi poprzez odwiedzenie strony domowej dostępnej pod adresem: **https://surfshark.com/pl**. Pamiętajcie, aby skorzystać ze specjalnej oferty dla Czytelników Komputer Świata, szczegóły znajdują się na stronie 16.

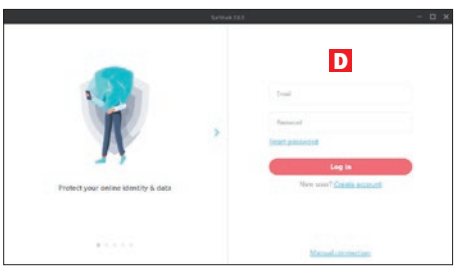


1 Po zakończeniu procesu rejestracji, zakupu i aktywacji usługi zostajemy przekierowani na stronę **Ustawienia konta** A. Nie musimy tu nic zmieniać, po lewej stronie okna przeglądarki klikamy kolejno na **VPN**, a następnie **Aplikacje i rozszerzenia** B.

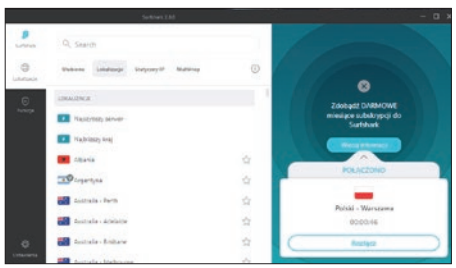




2 W grupie **Polecane** zobaczymy dwa elementy: link do aplikacji **Surfshark dla: Windows** C oraz program Surfshark w formie rozszerzenia dla używanej przeglądarki (w naszym przykładzie dla Google Chrome). Pobieramy program dla Windows, klikając na **Pobierz**.

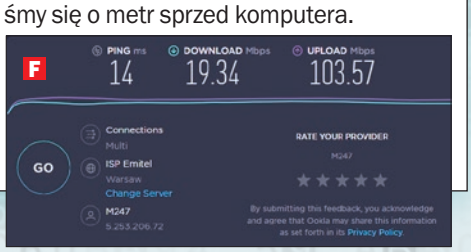


3 Po pobraniu aplikacji instalujemy ją, proces jest w pełni automatyczny. Gdy się zakończy, zobaczymy okienko logowania D, w którym logujemy się do usługi podanym wcześniej mailem i hasłem. Po zalogowaniu zaczynamy od zmiany języka, klikając na **Settings**, następnie **Language** i wybierając **Polski**. Aplikacja zażąda ponownego uruchomienia, zróbmy to, a będziemy mieć już polski interfejs.

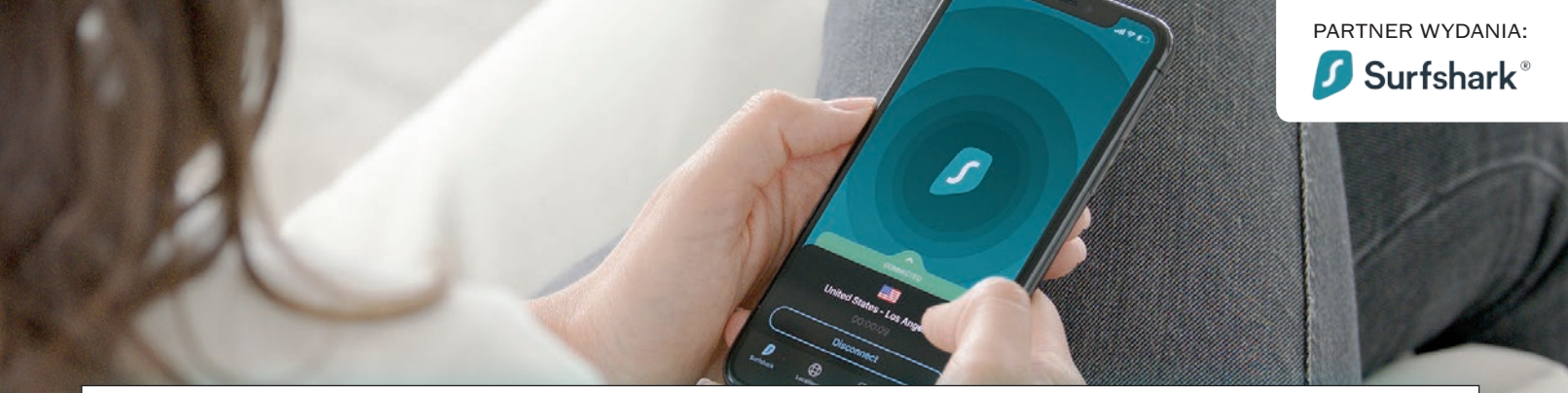


4 Po zalogowaniu i zmianie języka zobaczymy okienko z listą lokalizacji serwerów usługi SurfShark VPN. Na samej górze znajdują się opcje **Najszybszy serwer** oraz **Najbliższy kraj**. Wybieramy je, gdy zależy nam na anonimowym, ale też możliwie jak najszybszym surfowaniu. Klikamy na **Najszybszy serwer**.

5 Po krótkim sprawdzeniu szybkości dostępnych serwerów (trwa to kilka sekund) zostaniemy automatycznie połączeni z jednym z serwerów VPN. W naszym przypadku był to serwer również w Polsce, ale cel – zmiana naszego adresu IP – został osiągnięty. Różnice w szybkości pokazują poniższe dwa pomiary – jeden z nich E wykonaliśmy w redakcji bez aktywnego VPN, drugi pomiar to test szybkości łącza już po aktywacji VPN F. Zwróćcie uwagę na to, że test prędkości wykrywa nas jako zupełnie inny serwer, choć nie ruszyliśmy się o metr sprzed komputera.



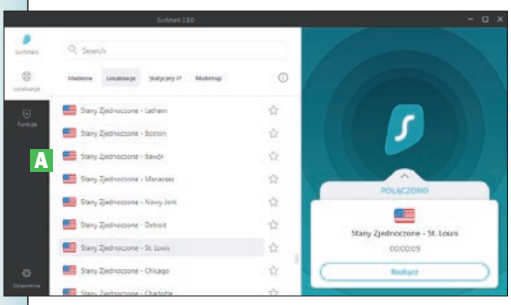
PARTNER WYDANIA:
Surfshark®



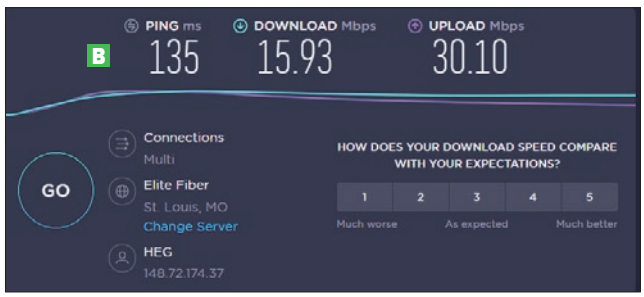
VPN NA KOMPUTERZE – WYBÓR LOKALIZACJI

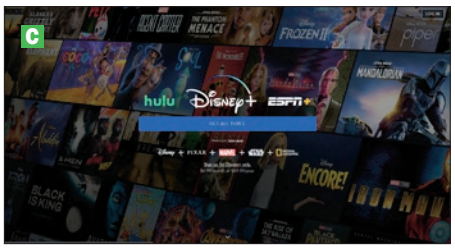
A co zrobić w przypadku, gdy chcemy, by odwiedzana przez nas strona uważała, że jesteśmy na przykład w Stanach Zjednoczonych? To bardzo proste.

1 W oknie programu Surfshark klikamy na **Lokalizacje**, a następnie wybieramy jeden z amerykańskich serwerów A obsługiwanych przez SurfShark. Podobnie jak wcześniej wystarczy po prostu kliknąć na lokalizację, a rozpocznie się test i inicjacja połączenia. Jeżeli z jednym serwerem się nie udaje, spróbujemy z innym, w tym samym kraju.



2 Na załączonej ilustracji jest przykład połączenia z jednym z serwerów w USA. Nie ruszyliśmy się zza biurka redakcyjnego, ale zdaniem odwiedzanych serwisów jesteśmy anonimowymi Amerykanami. Przeprowadziliśmy kolejny test prędkości, oto jego wynik B.



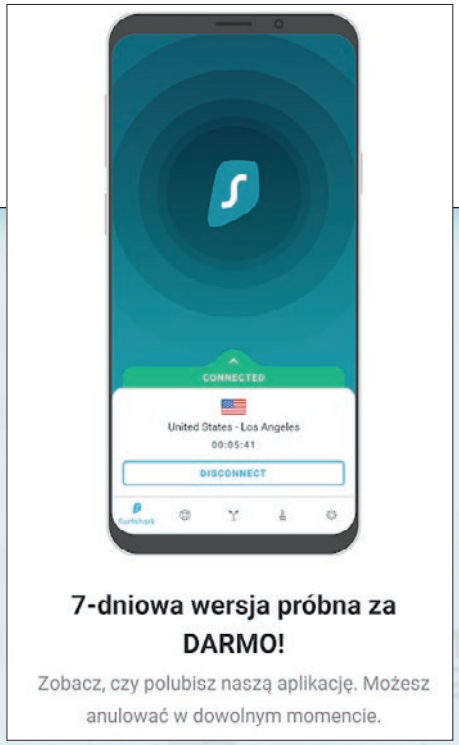


3 Jak widać, szybkość jest wciąż dobra, w zupełności wystarczająca na korzystanie z wielu niedostępnych w Polsce, amerykańskich usług online C.

VPN NA SMARTFONIE

Zajmijmy się teraz konfiguracją usługi SurfShark VPN na smartfonie z Androidem (w przypadku smartfonów Apple procedura wygląda bardzo podobnie, jedyną różnicą jest to, że stosowną apkę pobieramy ze sklepu App Store, a nie z Google Play).

1 Zaczynamy od zainstalowania na smartfonie aplikacji Surfshark VPN (**https://play.google.com/store/apps/details?id=com.surfshark.vpnclient.android**).



2 Po uruchomieniu aplikacji rezygnujemy z darmowej wersji próbnej. Pukamy w link **Masz już konto? Zaloguj się** i logujemy się do już zarejestrowanej wcześniej na komputerze usługi. Po zalogowaniu wystarczy nacis nąć **Połącz**, by podłączyć smartfon do najszybszego serwera VPN. Jeżeli analogicznie jak w przypadku połączenia na komputerze zechcemy się połączyć z serwerem zlokalizowanym w konkretnym kraju, pukamy w widoczną na dole ekranu aplikacji ikonę **Lokalizacje**.

OPCJONALNE FUNKCJE OCHRONNE

Za dodatkową opłatą 3,68 złotego miesięcznie usługa SurfShark VPN oferuje dwie dodatkowe funkcje:

- Surfshark Alert to system generujący automatyczne powiadomienie ostrzegawcze, gdy twój adres e-mail pojawi się w jakichkolwiek ujawnionych (na przykład w wyniku ataku hakerskiego) bazach danych.
- Surfshark Search jest dodatkowym zabezpieczeniem podczas wyszukiwania informacji w internecie, pozwala wyszukiwać bez profilowania użytkownika.

SURFSHARK VPN NA TV, KONSOLI, CHROMECAŚCIE

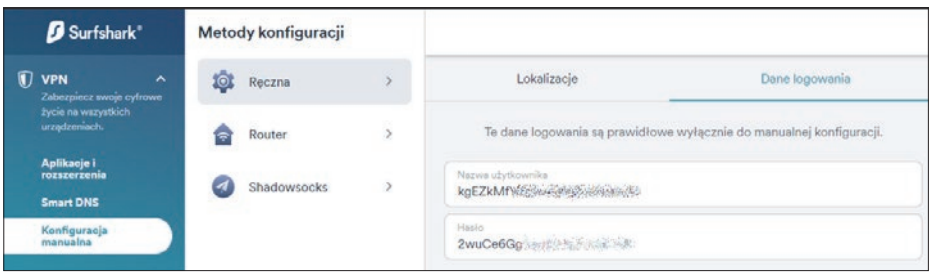
Komputer czy smartfon to nie wszystkie urządzenia, z których korzystamy w domowej sieci. Wielu korzysta także z ***telewizora smart, Chromecasta czy konsoli do gier.*** ***Na tych sprzętach także można używać VPN.*** *Zobaczmy, jak skorzystać z tej możliwości*

W wypadku niektórych routerów możliwe jest takie ich skonfigurowanie, by cały ruch naszej sieci domowej transferowany był przez VPN. Urządzenia takie należą jednak do rzadkości, a konfiguracja nie jest najprostsza. Natomiast dysponując routerem, który dostarczają operatorzy internetu czy telewizji kablowej, praktycznie można zapomnieć o takiej możliwości. Jeśli jednak mamy odpowiednie urządzenie, nic nie stoi na przeszkodzie, by cały nasz ruch sieci domowej kierować przez VPN. Alternatywnie możemy w Windows 10 uruchomić dedykowany punkt dostępowy – zamiast z routerem nasze urządzenia połączymy z nim, by zabezpieczyć transmisję VPN-em. Drugie rozwiązanie jest ostatecznością, gdyż z uwagi na ograniczenia kart Wi-Fi w komputerach i laptopach na pewno doświadczymy spadków prędkości połączeń: tego nie da się przeskoczyć.

KONFIGURUJEMY ROUTER

Bezpośrednio do łączenia z VPN możemy wykorzystać routery używające oprogramowań: DD-WRT, AsusWRT, Tomato lub OpenWRT. Najłatwiej zrobimy to, wykonując po kolei punkty porad umieszczonych na stronie Surfshark. Do nawiązania połączenia będziemy jednak potrzebowali danych logowania (innych niż nasz login i hasło do Surf sharka) oraz adresu serwera VPN, z którym nawiążemy połączenie.

1 Otwieramy stronę my.surfshark.com/vpn/manual-setup/main. W lewej części okna klikamy na **Konfiguracja manualna**.



2 Nazwę użytkownika oraz hasło logowania znajdziemy po kliknięciu na **Dane logowania**. Zapisujemy widoczne dane najlepiej w pliku tekstowym, skąd łatwo będzie nam je ponownie skopiować.

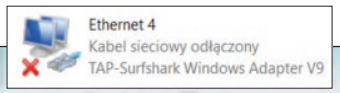
3 W lewej części okna klikamy na **Konfiguracja manualna**. Adres serwera kopiujemy z zakładki **Lokalizacje**. Zapisujemy widoczne dane – po uprzednim wybraniu lokalizacji serwera VPN.

4 Aby dotrzeć do poradników konfiguracyjnych routerów, klikamy na **Konfiguracja manualna**, potem na **Router** i w prawej części w sekcji Samouczki na nazwę oprogramowania używanego przez nasz router.

URUCHAMIAMY PUNKT DOSTĘPOWY W WINDOWS

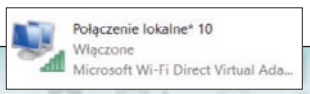
Jeśli nie dysponujemy odpowiednim sprzętem, pozostaje nam skonfigurować komputer z systemem Windows, by pełnił rolę routera VPN, przez który inne urządzenia będą nawiązywać połączenie. Ta metoda zadziała w wypadku każdego urządzenia, które podłączymy do utworzonego punktu dostępowego: smart TV, konsoli, Chromecasta.

1 Prawym przyciskiem myszy klikamy na ikonę połączenia kablowego lub Wi-Fi w zasobniku systemowym i wybieramy **Otwórz ustawienia sieci i Internetu**. Następnie klikamy na **Zmień opcje karty**. W nowym oknie odszukujemy i zapamiętujemy nazwę połączenia z **TAP-Surfshark** w nazwie (w przykładzie – Ethernet 4).



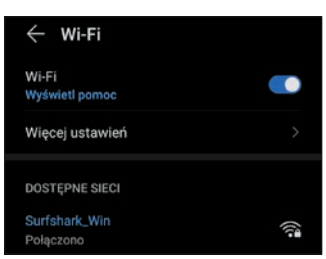
2 W otworzonym wcześniej oknie ustawień sieci i internetu klikamy na **Hotspot mobilny**. Klikamy na **Edytuj**, ustawiamy nazwę sieci zabezpieczonej przez VPN oraz hasło, po czym u góry okna przesuwamy przełącznik na pozycję **Włączone**. W oknie z punktu **1** pojawi się nam nowe połączenie z oznaczeniem Microsoft Wi-Fi Direct.

3 W oknie z punktu **1** klikamy prawym przyciskiem myszy na połączenie **TAP-Surfshark**, wybieramy **Właściwości**, przechodzimy na zakładkę **Udostępnianie**. Zaznaczamy opcję **Zezwalaj innym użytkownikom...**, a potem wybieramy z aktywowanej listy połączenie, które pojawiło się po wykonaniu punktu **2**. Klikamy na **OK**.



4 Teraz w aplikacji Surf shark klikamy na **Ustawienia**, **Zaawansowane**. W sekcji **Protokół** wybieramy **OpenVPN (UDP)**. Następnie łączymy się z siecią VPN na komputerze.

5 Następnie konfigurujemy Chromecast, konsolę lub smart TV do łączenia się z utworzonym punktem dostępu.



SURFSHARK VPN DODATKOWA OCHRONA

Opisana na poprzednich stronach usługa SurfShark VPN to nie tylko rozwiązanie pozwalające na anonimowe surfowanie po sieci, ale też ***sposób na monitorowanie, czy nasze dane nie padły łupem hakerów w wyniku skutecznego ataku na jakiś serwis internetowy****, w którym mieliśmy swoje konto. Podpowiadamy, jak z tego korzystać*

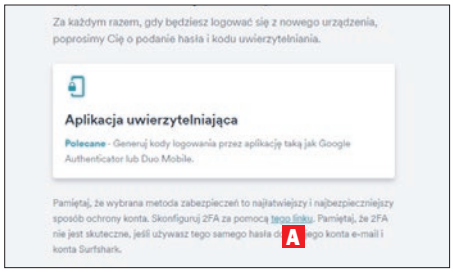
Zacznijmy od tego, że dostęp do dodatkowych funkcji w usłudze SurfShark, czyli monitorowania wycieków danych takich jak e-mail czy dane kart płatniczych, wymaga aktywacji dodatkowego pakietu Alert w samej usłudze. Jest on płatny niecałe 4 złote miesięcznie. Gdy uiścimy tę opłatę, obowiązkowo konieczne będzie jeszcze podniesienie poziomu bezpieczeństwa korzystania z samej usługi SurfShark VPN poprzez aktywację uwierzytelniania dwuskładnikowego. Od tego zaczniemy. Wszelkie operacje przeprowadzamy za pomocą przeglądarkowego interfejsu usługi dostępnego za pośrednictwem adresu **https://my.surfshark.com**.

AKTYWACJA UWIERZYTELNIANIA DWUSKŁADNIKOWEGO

Po wykupieniu dodatkowego pakietu usługi Alert i zatwierdzeniu warunków tej usługi w oknie przeglądarki zostaniemy poinformowani, że musimy włączyć uwierzytelnianie dwuskładnikowe.

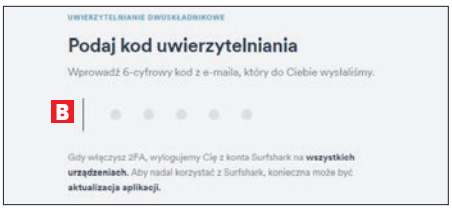
1 Na stronie **Włącz uwierzytelnianie dwuskładnikowe** klikamy na przycisk **Rozpocznij**.

2 W komunikacie na kolejnej stronie wybieramy widoczny w treści link „tego linku” **A**. Na kolejnej stronie zostaniemy poproszeni o wprowadzenie kodu, który został



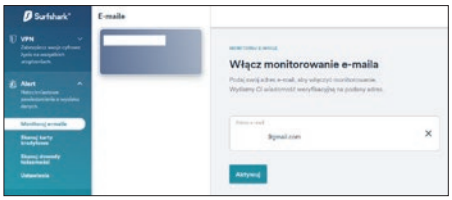
właśnie wysłany na e-mail podany podczas rejestracji w usłudze SurfShark VPN. Po wpisaniu kodu **B** klikamy na **Dalej**.

3 W kolejnym kroku wyświetlone zostaną unikalne dla naszego konta kody odzyskiwania, zapisujemy je, możemy je też pobrać (przycisk **Pobierz kody odzyskiwania**). Kody



są wyświetlane tylko ten jedyny raz. Jeżeli je stracimy, a w przyszłości na przykład utracimy dostęp do maila i do tych kodów, odzyskanie konta SurfShark nie będzie możliwe. Po zabezpieczeniu kodów klikamy na **Gotowe**.

MONITOROWANIE ADRESU E-MAIL

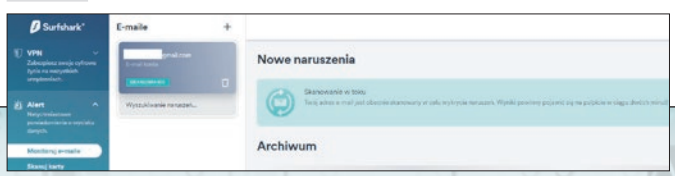


Pierwszą funkcją w ramach pakietu Alert w usłudze SurfShark VPN jest monitorowanie e-maila. Oto jak je włączyć.

1 W interfejsie przeglądarkowym usługi klikamy po lewej stronie na **Alert**, a następnie na **Monitoruj e-maile**. Ustawiając tę funkcję po raz pierwszy, adres użyty do rejestracji w SurfShark VPN będzie automatycznie dodany jako ten, który ma być monitorowany – jeżeli to akceptujemy, klikamy na przycisk **Aktywuj**.

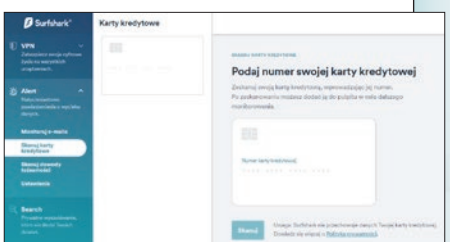
2 Przechodzimy teraz do swojej skrzynki e-mail, odbieramy wiadomość weryfikacyjną i postępujemy według zapisanych w niej wskazówek.

3 Po zweryfikowaniu adresu e-mail SurfShark rozpocznie analizę i skanowanie ewentualnych naruszeń, w których mógłby się pojawić nasz e-mail. Proces ten może potrwać kilka minut.



SKANOWANIE NARUSZEŃ KART PŁATNICZYCH

To kolejna funkcja bezpieczeństwa oferowana w ramach usługi SurfShark VPN. Działa podobnie do wspomnianej usługi monitorowania e-maila.



1 Z menu webowego interfejsu usługi po lewej stronie wybieramy pozycję **Alert** i **Skanuj karty kredytowe**.

2 W centralnej części okna w pole tekstowe wprowadzamy numer karty, którą chcemy sprawdzić pod kątem ewentualnych „wycieków” w internecie. Po wprowadzeniu numeru klikamy na widoczny na dole przycisk **Skanuj**. Również w tym przypadku wynik wymaga odrobiny cierpliwości.

Ważne: usługa nie przechowuje numerów skanowanych kart.

3 W przypadku nieznalezienia naruszeń bezpieczeństwa związanych z podanym numerem karty można kartę dodać do pulpitu usługi, dzięki czemu w razie gdyby gdziekolwiek w monitorowanych przez usługę bazach pojawił się ten numer, otrzymamy natychmiast powiadomienie.

Surfshark®

CHRONI CZYTELNIKÓW

83% *ZNIŻKI DLA CZYTELNIKÓW*

BEZ LIMITU *LICZBY URZĄDZEŃ*

PEŁNE SZYFROWANIE *DLA CAŁEJ SIECI DOMOWEJ*

ATAKI HAKERÓW

Złodzieje danych poszukują niezabezpieczonych urządzeń, a ci, którzy nie stosują szyfrowania, są łatwym celem ataków.

ZŁOŚLIWE OPROGRAMOWANIE I PHISHING

Te rodzaje ataków są powszechne i trudno uniknąć ich bez odpowiedniej ochrony.

KRADZIEŻ TOŻSAMOŚCI

Jeśli nie stosujesz oprogramowania zapewniającego bezpieczeństwo, twoje dane logowania mogą zostać skradzione.

MANIPULACJA ZA POMOCĄ REKLAM

Reklamodawcy mogą łatwo wpłynąć na twoje zachowanie, jeśli ujawnisz swoje wszystkie nawyki dotyczące przeglądania internetu.

ŚLEDZENIE ISP

Bez VPN twój dostawca usług internetowych może gromadzić i sprzedawać twoje dane reklamodawcom.

DYSKRYMINACJA CENOWA

Firmy online mogą oferować ci wyższe ceny, jeśli zobaczą, że znajdujesz się w bardziej zamożnym mieście.

- Wejdź na stronę **surfshark.deals/KS2021**
- Kliknij na **Kup teraz**
- Wybierz plan **24 miesiące + 3 bezpłatne**
- Zainstaluj Surfshark **na każdym urządzeniu**

Kod promocyjny **KS2021**, uprawniający do zniżki 83% oraz 3 miesięcy gratis przy zakupie abonamentu na 24 miesiące, jest aktywny do 1 maja 2021 roku.

Komputer Świat od 1998 roku

Adres redakcji: 02-672 Warszawa, ul. Domaniewska 49
internet: www.komputerswiat.pl, forum.komputerswiat.pl
e-mail: redakcja@komputerswiat.pl

Agnieszka Serafinowicz: autorka tekstów

Rafał Kamiński: redaktor naczelny
Tomasz Paczuski: z-ca redaktora naczelnego, szef wydania drukowanego
Agnieszka Al-Jawahiri: z-ca redaktora naczelnego, szef wydań specjalnych

Jolanta Rososińska: korekta
Robert Dobrzyński: dyrektor artystyczny
Mariusz Rybak: redaktor graficzny

ringier axel springer

Wydawca: RINGIER AXEL SPRINGER POLSKA Sp. z o.o.
Członek Izby Wydawców Prasy i Związku Kontroli Dystrybucji Prasy
www.ringieraxelspringer.pl, asp@axelspringer.pl
Adres: 02-672 Warszawa, ul. Domaniewska 49
tel. 22 2320000, 22 2320001

Prezes Zarządu: Mark Dekan
Prezes Honorowy: Wiesław Podkański
Dyrektor Generalny: Marcin Biegluk
Dyrektor Finansowy: Krzysztof Stopa
Dyrektor Sprzedaży: Mariusz Wąsiński
Dyrektor Marketingu: Olga Korolec

media impact

Biuro reklamy: Media Impact
reklama.warszawa@mediaimpact.pl
tel. (12) 2600200 (BOK)

Business Project Manager: Paweł Bulwan
Dział personalny: Monika Remiszewska
Księgowość: Katarzyna Fita (dyrektor)
Kolportaż: Rafał Kamiński (dyrektor)
Produkcja: Mariusz Gajda
Druk: Walstead Kraków Sp. z o.o.

Prenumerata i egzemplarze archiwalne:
www.literia.pl

Zdjęcie na okładce:
Nikita Gonin/123rf.com

Sprzedaż internetowa: www.literia.pl
Prenumerata zagraniczna: www.literia.pl
E-wydania: ksplus.pl

Redakcja nie zwraca materiałów niezamówionych, zastrzega sobie prawo redagowania nadesłanych tekstów, nie odpowiada za treść zamieszczanych reklam i ogłoszeń

Zabroniona jest bezumowna sprzedaż czasopisma po cenie niższej od ceny detalicznej ustalonej przez wydawcę. Sprzedaż numerów aktualnych i archiwalnych po innej cenie jest nielegalna i grozi odpowiedzialnością karną.